

An up-to-date version of this CV is always available here.



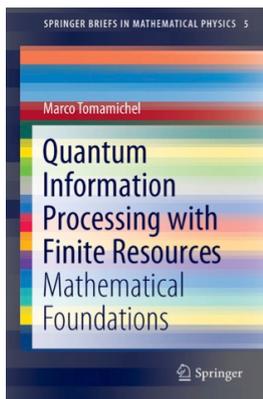
Marco Tomamichel
marco.tomamichel@nus.edu.sg
<http://www.marcotom.info>

Affiliation

Department of Electrical and Computer Engineering & Centre for Quantum Technologies
National University of Singapore

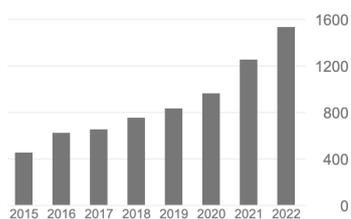
Research output

Published **76** journal articles (25 IEEE T-IT, 9 PRL, 4 CMP, 4 Nat. Comm., 1 Nat. Phys.) and 2 reviews (1 RMP), **33** conference proceedings, and a monograph



Bibliometrics

Total citations: 8114
h-Index: 44



Source: Google Scholar (January, 2023)

Marco Tomamichel

information theorist at the quantum frontier

About me My interests lie in the intersection of *cryptography*, *information theory* and *quantum mechanics*. I care deeply about the mathematical foundations of quantum information theory, for example the study of information measures, and about cryptography and communication in a world where quantum computers are emerging.

Since April 2020, Associate Professor

Department of Electrical and Computer Engineering, National University of Singapore

Since June 2020, Principal investigator

Centre for Quantum Technologies (CQT), National University of Singapore

Past positions

January 2017 – December 2018, Senior Lecturer and DECRA Fellow

January 2019 – April 2020, Associate Professor

School of Computer Science and Centre for Quantum Software and Information at University of Technology Sydney

July 2014 – December 2016, University of Sydney Postdoctoral Fellow

School of Physics at University of Sydney

March 2012 – June 2014, Research Fellow

Centre for Quantum Technologies at National University of Singapore

Education

2007–2012, ETH Zurich

Ph.D. in Physics; thesis: *A framework for non-asymptotic quantum information theory*

2002–2007, ETH Zurich

M.Sc. in Electrical Engineering and Information Technology, with ETH medal

Research highlights

2013, Article: *Quantum Rényi entropies: a new generalization and some properties.*

Journal of Mathematical Physics **54** (12), 122203 (2013)

- Introduces a new quantum generalisation of Rényi relative entropy that since has found various applications in quantum information.

2016, Article: *Quantum coding with finite resources*

Nature Communications **7**, 11419 (2016)

- We analyse the fundamental limits of quantum communication under the constraint that only small quantum devices are available for encoding and decoding.

2017, Article: *Multivariate trace inequalities*

Communications in Mathematical Physics **352** (1), 37–58 (2017).

- We improve upon the data-processing inequality for quantum entropy, one of the fundamental results in quantum information theory.
- Jack Keil Wolf ISIT Student Paper Award 2016 for student on the project

2020, Article: *Quantum advantage with noisy shallow circuits*

Nature Physics (2020), presented at FOCS 2019 and QIP 2020

- We propose a family of problems that are easy for noisy constant-depth quantum circuits, but can provably only be solved with a logarithmic-depth classical circuit. This is the first time such a gap has been shown conclusively.

2018, Article: *Quantum attacks on Bitcoin, and how to protect against them*

- We expose and analyse the vulnerability of cryptocurrencies (e.g. bitcoin) to attacks by quantum computers, and propose countermeasures.
- Global media attention (10+ articles, The Conversation, Altmetric score: 250+)

Other highlights

- Since 2019, Associate Editor for IEEE Transactions on Information Theory.
- Since 2022, on Editorial Board of Proceedings of the Royal Society A.
- 2018–2023, Local organisation of TQC, member and chair of steering committee.
- Programme committee QIP 2022&21&18, QCrypt 2023&21&19&17&14, ISIT 2015.
- 2022, Invited tutorial at QIP and invited talk at APS March Meeting.
- 2021, > \$1m SGD funding from Singapore's Quantum Engineering Programme.
- 2016–2020, Editor for Quantum, a community-driven open-access journal

Major research grants, fellowships and awards

2021, Quantum Engineering Programme (NRF2021-QEP2-01-P06)

Quantum homomorphic encryption: the Swiss army knife for the quantum internet? (Principle investigator (PI), \$896k SGD from National Research Foundation, Singapore)

2021, Quantum Engineering Programme (NRF2021-QEP2-02-P05)

Computer science approaches to quantum computing for finance. (Co-PI, ~\$300k SGD from National Research Foundation, Singapore)

2020, Discovery Project (DP200102273)

Securing the quantum internet with high-dimensional quantum systems, with Jacqui Romero and Andrew White at University of Queensland. (Co-PI, ~\$300k AUD granted by the Australian Research Council to UTS node, forfeited due to move)

2016–2019, Discovery Early Career Researcher Award

Information Processing with Small Quantum Devices. (\$320k AUD granted by the Australian Research Council, 16% success rate)

2014, University of Sydney Postdoctoral Fellowship

Practical Quantum Cryptography. (~\$250k granted by the University of Sydney)

2007, ETH Medal for outstanding Masters thesis

Microscopic Inhomogeneous Broadening Model for InGaN-based Semiconductor Laser Simulation

Other awards and fellowships

- 2022, Visiting Researcher at the Pauli Centre and Institute for Theoretical Physics at ETH Zurich, Switzerland.
- 2019, Finalist for UTS Research Leadership and Development Award.
- 2019–2020, Visiting Senior Research Fellow at the Centre for Quantum Technologies, Singapore.
- 2018, Fellow at the Stellenbosch Institute for Advanced Studies, South Africa.
- 2016, Jack Keil Wolf ISIT Student Paper Award 2016, awarded to David Sutter, on a project I supervised.
- 2016–, Senior Member of the IEEE Information Theory Society.
- 2016, Outstanding Reviewer, New Journal of Physics.
- 2013, Article included in Highlights of 2013 of the Journal of Physics A: Mathematical and Theoretical.
- 2006, Dean's list at Northwestern University, Evanston, Illinois, USA.
- 2003, Siemens Prize for Best *Vordiplom* (undergraduate exam) at the Department of Information Technology and Electrical Engineering, ETH Zurich.

Service to research community

Since 2019, Associate Editor for IEEE Transactions on Information Theory.

The leading journal on information theory.

Since 2022, on the Editorial Board of Proceedings of the Royal Society A.

Chair of the local organisation committee of TQC 2018; 2019–2021, member of the steering committee of TQC; 2021–2023, chair of the steering committee of TQC.

TQC is the second largest conference on the theory of quantum computing, cryptography and communication after QIP.

2016–2020, Editor for Quantum journal

A community-driven, non-profit and open-access journal for quality research in quantum information.

Programme committees

- QCrypt 2023 (Maryland, USA)
- Beyond I.I.D. 2023 (Tübingen, Germany) — **chair**
- QIP 2022 (Pasadena, USA)
- QIP 2021 (Munich, Germany)
- QCrypt 2021 (Amsterdam, The Netherlands)
- ITW 2021 (Kanazawa, Japan)
- QCrypt 2019 (Paris, France)
- QIP 2018 (Delft, Netherlands)
- QCrypt 2017 (Cambridge, UK)
- ISIT 2015 (Hong Kong, China)
- TQC 2015 (Brussels, Belgium)
- ICITS 2015 (Lugano, Switzerland)
- QCrypt 2014 (Paris, France)

University service

- 2022, Member of the University Senate Delegacy at NUS.
- 2020–2021, Coordinator for Quantum Engineering Programme (QEP 2.0) for the track Quantum Communication.
- 2022–2023, Conducting Graduate Student Admission Interviews.

Other service

- 2023, Member of StartupSG Tech Evaluation Panel, Enterprise Singapore.
- 2018, Organised workshop “Cryptography in the quantum age” at Stellenbosch Institute for Advanced Study.
- 2014, Chairing the organization of the second edition of the workshop “Beyond i.i.d. in information theory”; founding member of the steering committee of the conference series.
- 2012, Local organization committee of QCrypt 2012 in Singapore.
- 2014–2016, Mentor (yearly interviews) for Ph.D. candidates at the School of Physics.
- 2011, Organization of the NCCR/QSIT Junior-Meeting (a workshop for PhD students studying quantum information in Switzerland).
- 2005–2006, Student representative at departmental meetings, ETH Zurich.
- Reviewing (list not exclusive) for Nature Physics, Nature Communications, Physical Review Letters, IEEE Transactions on Information Theory, Physical Review A, New Journal of Physics, Communications in Mathematical Physics, Journal of Mathematical Physics.

Student supervision

Completed Masters/Ph.D. supervision

1. Dr. Hao-Chung Cheng, Ph.D. at the University of Technology Sydney (2018), co-supervision with Min-Hsieh Hsieh. Now Assistant Professor at National Taiwan University, Taiwan.
2. Dr. Christopher T. Chubb, Ph.D. at the University of Sydney (2019), co-supervision with Steven T. Flammia. Now Postdoc at ETH Zurich, Switzerland.
3. Dr. Akram Youssry, Ph.D. at the University of Technology Sydney (2020). Now Postdoc at Royal Melbourne Institute of Technology, Australia.

4. Alex McKinlay, Masters at the University of Technology Sydney (2021). Now in private industry in Sydney, Australia.
5. Maria Quadeer, Ph.D. at the University of Technology Sydney (2022), co-supervision with Christopher Ferrie. Now Postdoc at Nanyang Technological University, Singapore.

Ongoing supervision

- Josep Lumberras, Ph.D. student at Centre for Quantum Technologies, Singapore.
- Roberto Rubboli, Ph.D. student at Centre for Quantum Technologies, Singapore.
- Yanglin Hu, Ph.D. student at Centre for Quantum Technologies, Singapore.
- Enrique Cervero, Ph.D. student at Centre for Quantum Technologies, Singapore.
- Frits Verhagen, Ph.D. student at Centre for Quantum Technologies, Singapore.
- Jan Seyfried, Masters student at ETH Zurich, Switzerland.

I am also supervising several semester and final year projects.

Thesis committee (external)

- Aadil Oufkir (École Normale Supérieure de Lyon, 2023)
- Ernest Tan (ETH Zurich, 2021)
- Shima Bab Hadiashar (University of Waterloo, 2020)
- Hakop Pashavan (University of Sydney, 2019)

Selected lectures and talks

University teaching

- 2021, Lecturer and coordinator for “Quantum Communication and Cryptography”, an undergraduate module at the National University of Singapore (NUS).
- 2020–22, Lecturer and coordinator for “Information Theory for Communication Systems”, a graduate module at NUS. In 2021 redesigned as “Information Theory and its Applications”.
- 2020–22, Designed and taught a new module, “Blockchain Engineering”, an undergraduate module at NUS.
- 2019, Lecturer for “Data Structures and Algorithms”, an undergraduate module at the University of Technology Sydney (UTS).
- 2016, Lecturer for quantum mechanics in a Physics module for Engineers at the University of Sydney (USyd).
- 2015, Designed and lectured a graduate course titled “Protecting and Transmitting Quantum Information”, jointly with Steven T. Flammia at USyd.

Other teaching activities

- 2022, Invited tutorial lecture at QIP 2022: “From One-Shot to Asymptotic Quantum Information Theory”.
- 2022, Guest lectures (2 weeks) as part of the course “Advanced Topics in Quantum Information Theory” at ETH Zurich, covering quantum learning theory.
- 2022, Lectures at the MasterClass on Entropy Inequalities at the University of Copenhagen.
- 2018, “Introduction to quantum cryptography.” Lecture at UTS-Tsinghua Quantum Computer Science School.
- 2017, “Minicourse on quantum information theory”, a lecture series at the University of Auckland, New Zealand.

- 2014–2015, Tutorials for first year courses in physics and computational science at the University of Sydney.
- 2013, Lecturer for graduate seminar in quantum information at the National University of Singapore.
- 2012, Invited tutorial lecture: *Smooth min/max-entropies*. 2nd Annual Conference on Quantum Cryptography (QCrypt) in Singapore.

Talks accepted at QIP and TQC

QIP is the premier and most competitive conference in the field and features only the most important advances each year.

1. TQC 2023, “New additivity properties of the relative entropy of entanglement and its generalizations”.
2. TQC 2024, “Sequential Methods in Quantum Hypothesis Testing”.
3. QIP 2023, “On generalised quantum Stein’s lemmata and the reversibility of quantum resources”.
4. QIP 2022, “Fundamental limits on correlated catalytic transformations”.
5. QIP 2020, “Quantum advantage with noisy shallow circuits in 3D”.
6. QIP 2020, “An information-theoretic treatment of quantum dichotomies”.
7. QIP 2018, “Moderate deviation analysis for classical communication over quantum channels” and “Moderate deviation analysis and sphere-packing bounds for classical-quantum channels”.
8. QIP 2018, “On converse bounds for classical communication over quantum channels”.
9. QIP 2017, “Multivariate trace inequalities”.
10. QIP 2017, “Converse bounds for private communication over quantum channels”.
11. QIP 2016, “Strong converse and finite resource tradeoffs for quantum channels”.
12. QIP 2014, “A new quantum generalization of the Rényi divergence with applications to the strong converse in quantum channel coding”.
13. QIP 2013, “Hierarchy of information quantities for the finite block length analysis of quantum tasks”.
14. QIP 2012, “The link between uncertainty relations and non-locality”.
15. TQC 2011, “Towards a tight finite key analysis for BB84”.

Selected invited talks

This list is incomplete. Talks at conferences with proceedings are listed under publications.

- 2023, “Entanglement monogamy via multivariate trace inequalities”. Workshop on Entanglement Assisted Communication Networks, Taipei, Taiwan.
- 2022, “Communication in the age of noisy intermediate-scale quantum computers”. Keynote speech at NExT Forum: Quantum communication technology and applications, Taipei, Taiwan (online).
- 2022, “New additivity properties of the relative entropy of entanglement and its generalizations”. Quantum Resources workshop, Singapore.
- 2022, “Quantum Rényi divergence and beyond”. High Energy Theory Seminar at Perdue University.
- 2022, “Quantum Rényi divergence and beyond”. Conference celebrating the 100th anniversary of Rényi’s birth. Budapest, Hungary.
- 2022, “Catalytic Resource Transformations”. Quantum Information Theory and Mathematical Physics 2022, Budapest, Hungary.
- 2022, “Fault-tolerant quantum advantage with shallow circuits”. TEAM-NET Quantum Computing Colloquium,

- Poland (given online).
- 2022, “Multi-armed quantum bandits: Exploration versus exploitation when learning properties of quantum states”. APS March Meeting 2022, Chicago, IL, USA.
 - 2021, “Optimal Adaptive Strategies for Sequential Quantum Hypothesis Testing”. Bernoulli World Congress in Probability and Statistics, Seoul (held online).
 - 2021, “Fault-tolerant quantum advantage with shallow circuits”. NCTS Annual Theory Meeting, Taiwan (held online).
 - 2021, “Entanglement-assisted quantum capacity beyond the first order”. Munich quantum entanglement meeting, Munich, Germany (held online).
 - 2020, “Using a quantum advantage to show quantum computational supremacy”. 12th Annual Symposium of the Centre for Quantum Technologies, Singapore.
 - 2019, “Fault-tolerant quantum advantage with shallow circuits in 3D”. MACAO: First Workshop On Mathematics and Algorithms for Cryptographic Advanced Objects, Wollongong, Australia.
 - 2019, “Finite size effects and resonances in resource interconversion”. Banff workshop on Algebraic and Statistical ways into Quantum Resource Theories, Banff, Canada.
 - 2019, “Information Measures, Matrix Analysis, and Recoverability”. QuICS Seminar at the University of Maryland, USA.
 - 2019, “Fault-tolerant quantum advantage with shallow circuits”. SIQSE Invited Talk, Shenzhen Institute for Quantum Science and Engineering, Southern University of Science and Technology, China.
 - 2018, “How a quantum computer can steal your bitcoin”. Fellow seminar at the Stellenbosch Institute for Advanced Studies, Stellenbosch, South Africa.
 - 2018, “A tight upper bound for the third-order asymptotics of most discrete memoryless channels”. Seminar at the Centre for IoT and Telecommunications at The University of Sydney, Australia.
 - 2018, “Efficient online quantum state estimation using a matrix-exponentiated gradient method”. Seminar at TU Munich, Germany and ETH Zurich, Switzerland.
 - 2018, “Quantum Communication: From Basic Science to Engineering”. Invited talk at Australian Communications Theory Workshop (AusCTW 2018), Newcastle, Australia.
 - 2017, “Processing information with small quantum devices”. Seminar at the School of Physics, Monash University, Melbourne, Australia.
 - 2016, “Second-order asymptotics for the classical capacity of image-additive quantum channels”. American Physical Society March Meeting, Baltimore, Maryland.
 - 2016, “Characterizing a channel beyond Shannon’s capacity: an overview”. Workshop to celebrate Shannon’s 100th birthday, University of Technology Sydney.
 - 2016, Seminar: “Processing information with small quantum devices”. Seminar at Electrical & Computer Engineering Department, University of Michigan, USA.
 - 2016, Seminar: “Strengthened monotonicity of relative entropy via pinched Petz recovery map”. Preskill Group Meeting at Caltech, Pasadena, USA.
 - 2015, Seminar: “Processing information with small quantum devices”. Quantum Information Seminar at MIT, Cambridge, USA.
 - 2015, “Asymptotic and non-asymptotic fundamental limits for quantum communication”. Workshop on “Beyond i.i.d. in information theory” in Banff, Canada.
 - 2015, “Are current security proofs of quantum cryptography trustworthy?” Workshop “Trustworthy Quantum Information” in Ann Arbor, Michigan.
 - 2015, Faculty candidate seminar: “Processing information with small quantum devices”. Seminar at Electrical Engineering Department, Princeton University, USA.
 - 2014, “Strong Converse Bounds for Quantum Communication”. Centre of Excellence for Engineered Quantum Systems (EQUS) Meeting in Sydney, Australia.
 - 2014, Seminar: “How much information can we send through a quantum channel in practice?” Seminar at Télécom ParisTech, France.
 - 2014, “Strong converse bounds for quantum communication”. Australia-Japan Workshop on Multi-user Quantum Networks in Sydney, Australia.
 - 2013, “Non-asymptotic fundamental limits and Gaussian approximations for classical-quantum channels”. Workshop on Mathematical Challenges in Quantum Information at the Isaac Newton Institute for Mathematical Sciences in Cambridge, England.
 - 2013, “Entropic uncertainty relations and their applications in quantum cryptography”. International Conference on Information Theoretic Security (ICITS 2013) in Singapore.
 - 2013, “A hierarchy of information quantities for finite block length analysis of quantum tasks”. Workshop on “Beyond i.i.d. in information theory” in Cambridge, England.
 - 2012, Seminar: “The link between uncertainty relations and non-locality”. CQIF Seminar at University of Cambridge, UK.
 - 2011, “The uncertainty principle and its applications to quantum key distribution”. QKD Post-Processing Workshop in Vienna, Austria.

Complete list of publications

Monographs

- M. Tomamichel. *Quantum information processing with finite resources — Mathematical foundations*. Volume 5 of SpringerBriefs in Mathematical Physics (Springer, 2016).

Review articles

1. S. Pirandola, U.L. Andersen, L. Banchi, M. Berta, D. Bunandar, R. Colbeck, D. Englund, T. Gehring, C. Lupo, C. Ottaviani, J. Pereira, M. Razavi, J. Shamsul Shaari, M. Tomamichel, V.C. Usenko, G. Vallone, P. Villoresi, P. Wallden. *Advances in Quantum Cryptography*. *Advances in Optics and Photonics* **12**(4), 1012–1236 (2020).
2. P.J. Coles, M. Berta, M. Tomamichel, S. Wehner. *Entropic uncertainty relations and their applications*. *Reviews in Modern Physics* **89** (1), 180504 (2017).

Journal articles

1. M. Cao, M. Tomamichel. *Comments on “Channel Coding Rate in the Finite Blocklength Regime”: On the Quadratic Decaying Property of the Information Rate Function*. *IEEE Transactions on Information Theory* **69**(9), 5528–5531 (2023).
2. Y. Ouyang, K. Goswami, J. Romero, B.C. Sanders, M.-H. Hsieh, M. Tomamichel. *Approximate reconstructibility of quantum states and noisy quantum secret sharing schemes*. *Physical Review A* **108**, 012425 (2023).
3. N. Ramakrishnan, M. Tomamichel, M. Berta. *Moderate deviation expansion for fully quantum tasks*. *IEEE*

- Transactions on Information Theory **69**(8), 5041–5059 (2023).
4. Y. Hu, Y. Ouyang, M. Tomamichel. *Privacy and correctness trade-offs for information-theoretically secure quantum homomorphic encryption*. Quantum **7**, 976 (2023).
 5. M. Rambach, A. Youssry, M. Tomamichel, J. Romero. *Efficient Quantum State Tracking in Noisy Environments*. Quantum Science and Technology **8**(1), 015010 (2022).
 6. R. Rubboli, M. Tomamichel. *Fundamental Limits on Correlated Catalytic State Transformations*. Physical Review Letters **129**, 120506 (2022).
 7. J. Lumbrellas, E. Haapasalo, M. Tomamichel. *Multi-armed quantum bandits: Exploration versus exploitation when learning properties of quantum states*. Quantum **6**, 749 (2022).
 8. K. Korzekwa, Z. Puchała, M. Tomamichel, K. Życzkowski. *Encoding classical information into quantum resources*. IEEE Transactions on Information Theory **68**(7), 4518–4530 (2022).
 9. Y. Li, V.Y.F. Tan, M. Tomamichel. *Optimal adaptive strategies for sequential quantum hypothesis testing*. Communications in Mathematical Physics **392**, 993–1027 (2022).
 10. G. Gour, M. Tomamichel. *Entropy and relative entropy from information-theoretic principles*. IEEE Transactions on Information Theory **67**(10), 6313–6327 (2021).
 11. M. Quadeer, K. Korzekwa, M. Tomamichel. *Work fluctuations due to partial thermalizations in two-level systems*. Physical Review E **103**(4), 042141 (2021).
 12. G. Gour, M. Tomamichel. *Optimal Extensions of Resource Measures and their Applications*. Physical Review A **102**, 062401 (2020).
 13. S. Bravyi, D. Gosset, R. König, M. Tomamichel. *Quantum advantage with noisy shallow circuits*. Nature Physics (2020).
 14. A. McKinlay, M. Tomamichel. *Decomposition Rules for Quantum Rényi Mutual Information with an Application to Information Exclusion Relations*. Journal of Mathematical Physics **61**, 072202 (2020).
 15. A. Anshu, M. Berta, R. Jain, M. Tomamichel. *Partially smoothed information measures*. IEEE Transactions on Information Theory **66**(8), 5022–5036 (2020).
 16. S. Huber, R. König, M. Tomamichel. *Jointly constrained semidefinite bilinear programming with an application to Dobrushin curves*. IEEE Transactions on Information Theory **66**(5), 2934–2950 (2020).
 17. K. Fang, X. Wang, M. Tomamichel, M. Berta. *Quantum channel simulation and the channel’s smooth max-information*. IEEE Transactions on Information Theory **66**(4), 2129–2140 (2020).
 18. A. Youssry, R.J. Chapman, A. Peruzzo, C. Ferrie, M. Tomamichel. *Modeling and control of a reconfigurable photonic circuit using deep learning*. Quantum Science and Technology **5**(2), 025001 (2020).
 19. A. Anshu, M. Berta, R. Jain, M. Tomamichel. *A Minimax approach to one-shot entropy inequalities*. Journal of Mathematical Physics **60**, 12221 (2019).
 20. F. Buscemi, D. Sutter, M. Tomamichel. *An information-theoretic treatment of quantum dichotomies*. Quantum Journal **3**, 209 (2019).
 21. K. Fang, X. Wang, M. Tomamichel, R. Duan. *Non-asymptotic entanglement distillation*. IEEE Transactions on Information Theory **65**(10), 6454–6465 (2019).
 22. X. Wang, K. Fang, M. Tomamichel. *On converse bounds for classical communication over quantum channels*. IEEE Transactions on Information Theory **65**(7), 4609–4619 (2019).
 23. P. Taranto, F.A. Pollock, S. Milz, M. Tomamichel, K. Modi. *Quantum Markov order*. Physical Review Letters **112**, 140401 (2019).
 24. K. Korzekwa, C.T. Chubb, M. Tomamichel. *Avoiding irreversibility: engineering resonant conversions of quantum resources*. Physical Review Letters **112**, 110403 (2019).
 25. C.T. Chubb, M. Tomamichel, K. Korzekwa. *Moderate deviation analysis of majorisation-based resource interconversion*. Physical Review A **99**, 032332 (2019).
 26. H.-C. Cheng, M.-H. Hsieh, M. Tomamichel. *Quantum sphere-packing bounds with polynomial prefactors*. IEEE Transactions on Information Theory **65**(5), 2872–2898 (2019).
 27. M. Quadeer, M. Tomamichel, C. Ferrie. *Minimax quantum state estimation under Bregman divergence*. Quantum **3**, 126 (2019).
 28. A. Youssry, C. Ferrie, M. Tomamichel. *Efficient online quantum state estimation using a matrix-exponentiated gradient method*. New Journal of Physics **21**, 033006 (2019).
 29. C.T. Chubb, M. Tomamichel, K. Korzekwa. *Beyond the thermodynamic limit: finite-size corrections to state interconversion rates*. Quantum **2**, 108 (2018).
 30. M. Berta, V.B. Scholz, M. Tomamichel. *Rényi divergences as weighted non-commutative vector valued L_p -spaces*. Annales Henri Poincaré **19**(6), 1843–1867 (2018).
 31. D. Aggarwal, G.K. Brennen, T. Lee, M. Santha, M. Tomamichel. *Quantum attacks on Bitcoin, and how to protect against them*. Ledger **3** (2018).
 32. M. Tomamichel, M. Hayashi. *Operational interpretation of Rényi information measures via composite hypothesis testing against product and Markov distributions*. IEEE Transactions on Information Theory **64**(2), 1064–1082 (2018).
 33. R.J. Chapman, A. Karim, Z. Huang, S.T. Flammia, M. Tomamichel, A. Peruzzo. *Beating the classical limits of information transmission using a quantum decoder*. Physical Review A, **97**, 012315 (2018).
 34. C. Pfister, M.A. Rol, A. Mantri, M. Tomamichel, S. Wehner. *Capacity estimation and verification of quantum channels with arbitrarily correlated errors*. Nature Communications **9**, 27 (2018).
 35. M. Berta, O. Fawzi, M. Tomamichel. *On variational expressions for quantum relative entropies*. Letters in Mathematical Physics **107**(12), 2239–2265 (2017).
 36. C.T. Chubb, V.Y.F. Tan, M. Tomamichel. *Moderate deviation analysis for classical communication over quantum channels*. Communications in Mathematical Physics **355**(3), 1562–1572 (2017).
 37. H.-C. Cheng, M.-H. Hsieh, M. Tomamichel. *Exponential decay of matrix Φ -entropies on Markov semigroups with applications to dynamical evolutions of quantum ensembles*. Journal of Mathematical Physics **58**(9), 092202 (2017).
 38. M.M. Wilde, M. Tomamichel, S. Lloyd, M. Berta. *Gaussian hypothesis testing and quantum illumination*. Physical Review Letters **119**(12), 120501 (2017).
 39. M. Tomamichel, A. Leverrier. *A largely self-contained and complete security proof for quantum key distribution*. Quantum **1**, 14 (2017).
 40. F. Hiai, R. König, M. Tomamichel. *Generalized log-*

- majorization and multivariate trace inequalities. *Annales Henri Poincaré* **18** (7), 2499–2521 (2017).
41. M.M. Wilde, M. Tomamichel, M. Berta. *Converse bounds for private communication over quantum channels*. *IEEE Transactions on Information Theory* **63** (3), 1792–1817 (2017).
 42. D. Sutter, M. Berta, M. Tomamichel. *Multivariate trace inequalities*. *Communications in Mathematical Physics* **352** (1), 37–58 (2017).
 43. M. Tomamichel, M.M. Wilde, A. Winter. *Strong converse bounds for quantum communication*. *IEEE Transactions on Information Theory* **63** (1), 715–727 (2017).
 44. M. Hayashi, M. Tomamichel. *Correlation detection and an operational interpretation of the Rényi mutual information*. *Journal of Mathematical Physics* **57**, 102201 (2016).
 45. C. Pfister, J. Kaniewski, M. Tomamichel, A. Mantri, R. Schmucker, N. McMahon, G. Milburn, S. Wehner. *A universal test for gravitational decoherence*. *Nature Communications* **7**, 13022 (2016).
 46. N. Datta, M. Tomamichel, M.M. Wilde. *On the second-order asymptotics for entanglement-assisted communication*. *Quantum Information Processing* **15** (6), 2569–2591 (2016).
 47. M. Tomamichel, M. Berta, J.M. Renes. *Quantum coding with finite resources*. *Nature Communications* **7**, 11419 (2016).
 48. D. Sutter, M. Tomamichel, A.W. Harrow. *Strengthened monotonicity of relative entropy via pinched Petz recovery map*. *IEEE Transactions on Information Theory* **62** (6), 2907–2913 (2016).
 49. M. Berta, M. Tomamichel. *The fidelity of recovery is multiplicative*. *IEEE Transactions on Information Theory* **62** (4), 1758–1763 (2016).
 50. T. Lunghi, J. Kaniewski, F. Bussières, R. Houlmann, M. Tomamichel, S. Wehner, H. Zbinden. *Practical relativistic bit commitment*. *Physical Review Letters* **115**(3), 030502 (2015).
 51. V.Y.F. Tan, M. Tomamichel. *The third-order term in the normal approximation for the AWGN channel*. *IEEE Transactions on Information Theory* **61** (5), 2430–2438 (2015).
 52. M. Tomamichel, V.Y.F. Tan. *Second-order asymptotics for the classical capacity of image-additive quantum channels*. *Communications in Mathematical Physics*, **338** (1), 103–137 (2015).
 53. S.M. Lin, M. Tomamichel. *Investigating properties of a family of quantum Rényi divergences*. *Journal of Quantum Information Processing* **14** (4), 1501–1512 (2015).
 54. M. Berta, M. Christandl, F. Furrer, V.B. Scholz, M. Tomamichel. *Position-momentum uncertainty relations in the presence of quantum memory*. *Journal of Mathematical Physics* **55** (12), 122205 (2014).
 55. M. Tomamichel, M. Berta, M. Hayashi. *Relating different quantum generalizations of the conditional Rényi entropy*. *Journal of Mathematical Physics* **55** (8), 082206 (2014).
 56. J. Kaniewski, M. Tomamichel, S. Wehner. *Entropic uncertainty from effective anticommutators*. *Physical Review A* **90** (1), 012332 (2014).
 57. M. Tomamichel, and V.Y.F. Tan. *Second-order coding rates for channels with state*. *IEEE Transactions on Information Theory* **60** (8), 4427–4448 (2014).
 58. F. Dupuis, O. Szechr, and M. Tomamichel. *A decoupling approach to classical data transmission over quantum channels*. *IEEE Transactions on Information Theory* **60** (3), 1562–1572 (2014).
 59. M. Müller-Lennert, F. Dupuis, O. Szechr, S. Fehr, and M. Tomamichel. *On Quantum Rényi entropies: a new generalization and some properties*. *Journal of Mathematical Physics* **54** (12), 122203 (2013).
 60. M. Tomamichel, S. Fehr, J. Kaniewski, and S. Wehner. *A monogamy-of-entanglement game with applications to device-independent quantum cryptography*. *New Journal of Physics* **15**, 103002 (2013).
 61. M. Tomamichel, V.Y.F. Tan. *A tight upper bound for the third-order asymptotics for most discrete memoryless channels*. *IEEE Transactions on Information Theory* **59** (11), 7041–7051 (2013).
 62. T. Lunghi, J. Kaniewski, F. Bussières, R. Houlmann, M. Tomamichel, A. Kent, N. Gisin, S. Wehner, and H. Zbinden. *Experimental bit commitment based on quantum communication and special relativity*. *Physical Review Letters* **111**, 042301 (2013).
 63. M. Tomamichel, and M. Hayashi. *A hierarchy of information quantities for finite block length analysis of quantum tasks*. *IEEE Transactions on Information Theory* **59** (11), 7693–7710 (2013).
 64. J. Kaniewski, M. Tomamichel, E. Hänggi, and S. Wehner. *Secure bit commitment from relativistic constraints*. *IEEE Transactions on Information Theory* **59** (7), 4687–4699 (2013).
 65. O. Szechr, F. Dupuis, M. Tomamichel, and R. Renner. *Decoupling with unitary approximate two-designs*. *New Journal of Physics* **15**, 053022 (2013).
 66. C.C.W. Lim, C. Portmann, M. Tomamichel, R. Renner, and N. Gisin. *Device-independent quantum key distribution with local Bell test*. *Physical Review X* **3**, 031006 (2013).
 67. A. Vitanov, F. Dupuis, M. Tomamichel, and R. Renner. *Chain rules for smooth min- and max-entropies*. *IEEE Transactions on Information Theory* **59** (5), 2603–2612 (2013).
 68. M. Tomamichel, and E. Hänggi. *The link between uncertainty relations and non-locality*. *Journal of Physics A: Mathematical and Theoretical* **46**, 055301 (2013).
 69. F. Furrer, T. Franz, M. Berta, V.B. Scholz, M. Tomamichel, and R. F. Werner. *Continuous Variable Quantum Key Distribution: Finite-Key Analysis of Composable Security against Coherent Attacks*. *Physical Review Letters* **109**, 100502 (2012).
 70. M. Tomamichel, C.C.W. Lim, N. Gisin, and R. Renner. *Tight finite-key analysis for quantum cryptography*. *Nature Communications* **3**, 634 (2012).
 71. M. Tomamichel, and R. Renner. *Uncertainty relation for smooth entropies*. *Physical Review Letters* **106**, 110506 (2011).
 72. M. Tomamichel, C. Schaffner, A. Smith, and R. Renner. *Leftover hashing against quantum side information*. *IEEE Transactions on Information Theory* **57** (8), 5524–5535 (2011).
 73. S. Winkler, M. Tomamichel, S. Hengli, and R. Renner. *Impossibility of growing quantum bit commitments*. *Physical Review Letters* **107**, 090502 (2011).
 74. M. Tomamichel, R. Colbeck, and R. Renner. *Duality between smooth min- and max-entropies*. *IEEE Transactions on Information Theory* **56** (9), 4674–4681 (2010).
 75. M. Tomamichel, R. Colbeck, and R. Renner. *A fully quantum asymptotic equipartition property*. *IEEE Transactions on Information Theory* **55** (12), 5840–5847 (2009).

(2009).

76. B. Witzigmann, M. Tomamichel, S. Steiger, R. G. Veprek, K. Kojima, and U. T. Schwarz. *Analysis of gain and luminescence in violet and blue GaInN–GaN quantum wells*. IEEE Journal of Quantum Electronics **44** (2), 144–149 (2008).

Refereed conference proceedings

1. C. Hirche, X. Guan, M. Tomamichel. *Chain Rules for Renyi Information Combining*. Proceedings of the IEEE International Symposium on Information Theory (ISIT 2023), 204–209 (Taipei, Taiwan, 2023).
2. M.X. Cao, N. Ramakrishnan, M. Berta, M. Tomamichel. *Broadcast Channel Simulation* Proceedings of the IEEE International Symposium on Information Theory (ISIT 2023), 1430–1435 (Taipei, Taiwan, 2023).
3. M. Berta, M. Tomamichel. *Chain rules for quantum channels*. Proceedings of the IEEE International Symposium on Information Theory (ISIT 2022), 2427–2432 (Helsinki, Finland, 2022).
4. M.X. Cao, N. Ramakrishnan, M. Berta, M. Tomamichel. *One-shot point-to-point channel simulation*. Proceedings of the IEEE International Symposium on Information Theory (ISIT 2022), 796–801 (Helsinki, Finland, 2022).
5. Y. Li, C. Hirche, M. Tomamichel. *Sequential quantum channel discrimination*. Proceedings of the IEEE International Symposium on Information Theory (ISIT 2022), 270–275 (Helsinki, Finland, 2022).
6. Y. Ouyang, M. Tomamichel. *Learning quantum graph states with product measurements*. Proceedings of the IEEE International Symposium on Information Theory (ISIT 2022), 2963–2968 (Helsinki, Finland, 2022).
7. Y. Li, V.Y.F. Tan, M. Tomamichel. *Optimal adaptive strategies for sequential quantum hypothesis testing*. Proceedings of the IEEE Information Theory Workshop (ITW 2021), 1–6 (Kanazawa, Japan, 2021).
8. N. Ramakrishnan, M. Tomamichel, M. Berta. *Moderate deviation analysis for quantum state transfer*. Proceedings of the IEEE Information Theory Workshop (ITW 2021), 1–6 (Kanazawa, Japan, 2021).
9. S. Bravyi, D. Gosset, R. König, M. Tomamichel. *Quantum advantage with noisy shallow circuits in 3D*. Proceedings of the IEEE Annual Symposium on Foundations of Computer Science (FOCS 2019), 995–999 (Baltimore, USA, 2019).
10. A. Anshu, M. Berta, R. Jain, M. Tomamichel. *Second-order characterizations via partial smoothing*. Proceedings of the IEEE International Symposium on Information Theory (ISIT 2019), 937–941 (Paris, France, 2019).
11. C.T. Chubb, K. Korzekwa, M. Tomamichel. *Moderate deviation analysis of majorisation-based resource interconversion*. Proceedings of the IEEE International Symposium on Information Theory (ISIT 2019), 3002–3006 (Paris, France, 2019).
12. K. Fang, X. Wang, M. Tomamichel, M. Berta. *Quantum channel simulation and the channel’s smooth max-information*. Proceedings of the IEEE International Symposium on Information Theory (ISIT 2018), 2326–2330 (Denver, USA, 2018).
13. X. Wang, K. Fang, M. Tomamichel. *On finite blocklength converse bounds for classical communication over quantum channels*. Proceedings of the IEEE International Symposium on Information Theory (ISIT 2018), 2157–2161 (Denver, USA, 2018).
14. H.-C. Cheng, M.-H. Hsieh, M. Tomamichel. *Sphere-packing bound for classical-quantum channels*. Proceedings of the IEEE Information Theory Workshop (ITW 2017), 479–483 (Kaohsiung, Taiwan, 2017).
15. H.-C. Cheng, M.-H. Hsieh, M. Tomamichel. *Sphere-packing bound for symmetric classical-quantum channels*. Proceedings of the IEEE International Symposium on Information Theory (ISIT 2017), 286–290 (Aachen, Germany, 2017).
16. M.M. Wilde, M. Tomamichel, M. Berta. *A meta-converse for private communication over quantum channels*. Proceedings of the IEEE International Symposium on Information Theory (ISIT 2017), 291–295 (Aachen, Germany, 2017).
17. C. Chubb, V.Y.F. Tan, M. Tomamichel. *Moderate deviation analysis for classical communication over quantum channels*. Proceedings of the IEEE International Symposium on Information Theory (ISIT 2017), 1544–1548 (Aachen, Germany, 2017).
18. D. Sutter, M. Berta, M. Tomamichel. *Quantum Markov chains and logarithmic trace inequalities*. Proceedings of the IEEE International Symposium on Information Theory (ISIT 2017), 1988–1992 (Aachen, Germany, 2017).
19. D. Sutter, M. Tomamichel, A. W. Harrow. *Strengthened monotonicity of relative entropy via pinched Petz recovery map*. Proceedings of the IEEE International Symposium on Information Theory (ISIT 2016), 760–764 (Barcelona, Spain, 2016). **(This submission received the Jack Keil Wolf ISIT Best Student Paper Award.)**
20. M. Tomamichel, M. Hayashi. *Operational interpretation of Rényi conditional mutual information via composite hypothesis testing against Markov distributions*. Proceedings of the IEEE International Symposium on Information Theory (ISIT 2016), 585–589 (Barcelona, Spain, 2016).
21. M. Berta, O. Fawzi, M. Tomamichel. *Exploiting variational formulas for quantum relative entropy*. Proceedings of the IEEE International Symposium on Information Theory (ISIT 2016), 2844–2848 (Barcelona, Spain, 2016).
22. M. Tomamichel, M.M. Wilde, A. Winter. *Strong converse rates for quantum communication*. Proceedings of the IEEE International Symposium on Information Theory (ISIT 2015), 2386–2390 (Hong Kong, China, 2015). *(presented as semi-plenary talk)*
23. M. Hayashi, M. Tomamichel. *Correlation detection and an operational interpretation of the Rényi mutual information*. Proceedings of the IEEE International Symposium on Information Theory (ISIT 2015), 1447–1451 (Hong Kong, China, 2015). *(presented as semi-plenary talk)*
24. N. Datta, M. Tomamichel, M.M. Wilde. *Second-order coding rates for entanglement-assisted communication*. Proceedings of the IEEE International Symposium on Information Theory (ISIT 2015), 2772–2776 (Hong Kong, China, 2015).
25. M. Tomamichel, J. Martinez-Mateo, C. Pacher, D. Elkouss. *Fundamental finite key limits for information reconciliation in quantum key distribution*. Proceedings of the IEEE International Symposium on Information Theory (ISIT 2014), 1469–1473 (Honolulu, USA, 2014).
26. M. Tomamichel, M. Berta, M. Hayashi. *A duality relation connecting different quantum generalizations of*

the conditional Rényi entropy. Proceedings of the IEEE International Symposium on Information Theory (ISIT 2014), 731–735 (Honolulu, USA, 2014).

27. V.Y.F. Tan, [M. Tomamichel](#). *The third-order term in the normal approximation for the AWGN channel*. Proceedings of the IEEE International Symposium on Information Theory (ISIT 2014), 2077–2081 (Honolulu, USA, 2014).
28. [M. Tomamichel](#), V.Y.F. Tan. *Second-order refinements for the classical capacity of quantum channels with separable input states*. Proceedings of the IEEE International Symposium on Information Theory (ISIT 2014), 141–145 (Honolulu, USA, 2014).
29. [M. Tomamichel](#), and V.Y.F. Tan. *ϵ -capacities and strong converse for channels with general state*. Proceedings of the Information Theory Workshop (ITW 2013), 1–5 (Seville, Spain, 2013)
30. [M. Tomamichel](#), S. Fehr, J. Kaniewski, and S. Wehner. *One-sided device-independent QKD and position-based cryptography from monogamy games*. Advances in Cryptology — EUROCRYPT 2013, 609–625 (Athens, Greece, 2013).
31. [M. Tomamichel](#), V.Y.F. Tan. *A tight upper bound for the third-order asymptotics of discrete memoryless channels*. Proceedings of the IEEE International Symposium on Information Theory (ISIT 2013), 1536–1540 (Istanbul, Turkey, 2013).
32. [M. Tomamichel](#), C. Schaffner, A. Smith, R. Renner. *Left-over hashing against quantum side information*. Proceedings of the IEEE International Symposium on Information Theory (ISIT 2010), 2703–2707 (Austin, USA, 2010).
33. O.G. Memis, S.C. Kong, A. Katsnelson, [M. Tomamichel](#), H. Mohseni. *A novel avalanche free single photon detector*. Proceedings of the IEEE Conference on Nanotechnology (NANO 2006), 724–745 (Cincinnati, USA, 2006).

Errata

- F. Furrer, T. Franz, M. Berta, V.B. Scholz, [M. Tomamichel](#), and R. F. Werner. *Erratum: Continuous Variable Quantum Key Distribution: Finite-Key Analysis of Composable Security Against Coherent Attacks*. Physical Review Letters **112** (1) 019902 (2014).

Thesis

- [M. Tomamichel](#). *A framework for non-asymptotic quan-*

tum information theory. Ph.D. Thesis, Institute for Theoretical Physics, ETH Zurich (2012). Available online at arXiv:1203.2142.

Preprints

1. R. Rubboli, R. Takagi, [M. Tomamichel](#). *Mixed-state additivity properties of magic monotones based on quantum relative entropies for single-qubit states and beyond*. Available online at arXiv:2307.08258 (2023).
2. C. Hirche, [M. Tomamichel](#). *Quantum Rényi and f -divergences from integral representations*. Available online at arXiv:2306.12343 (2023).
3. Y. Hu, [M. Tomamichel](#). *Fundamental limits on quantum cloning from the no-signalling principle*. Available online at arXiv:2305.02002 (2023).
4. M. Berta, [M. Tomamichel](#). *Entanglement monogamy via multivariate trace inequalities*. Available online at arXiv:2304.14878 (2023).
5. P. Lipka-Bartosik, C.T. Chubb, J.M. Renes, [M. Tomamichel](#), K. Korzekwa. *Quantum dichotomies and coherent thermodynamics beyond first-order asymptotics*. Available online at arXiv:2303.05524 (2023).
6. S. Brahmachari, J. Lumbrellas, [M. Tomamichel](#). *Quantum contextual bandits and recommender systems for quantum data*. Available online at arXiv:2301.13524 (2023).
7. M.U. Farooq, T. Fritz, E. Happasalo, [M. Tomamichel](#). *Asymptotic and catalytic matrix majorization*. Available online at arXiv:2301.07353 (2023).
8. M.X. Cao, N. Ramakrishnan, M. Berta, [M. Tomamichel](#). *Channel Simulation: Finite Blocklengths and Broadcast Channels*. Available online at arXiv:2212.11666 (2022).
9. R. Rubboli, [M. Tomamichel](#). *New additivity properties of the relative entropy of entanglement and its generalisations*. Available online at arXiv:2211.12804 (2022).
10. M. Berta, F.G.S.L. Brandão, G. Gour, L. Lami, M. B. Plenio, B. Regula, [M. Tomamichel](#). *On a gap in the proof of the generalised quantum Stein’s lemma and its consequences for the reversibility of quantum resources*. Available online at arXiv:2205.02813 (2022).

Popular books and media

1. [M. Tomamichel](#). “How quantum computers could steal your bitcoin”, The Conversation.
2. [M. Tomamichel](#), C. Ferrie. “Blockchain for Babies”, Sourcebooks (2019).